# CONGRESSIONAL BUDGET OFFICE
# COST ESTIMATE

March 30, 2006

# H.R. 3997
## Financial Data Protection Act of 2006

*As ordered reported by the House Committee on Financial Services*
*on March 16, 2006*

## SUMMARY

H.R. 3997 would require private companies with access to consumers' personal information to take certain precautions to safeguard that information. Private companies also would be required to notify consumers and certain authorities whenever there is a breach in the security of a consumer's personal information and to investigate and take steps to repair the breach. Under the bill, consumers would have the option of freezing their credit reports in the event of a threat to the security of their personal information. H.R. 3997 would require the Federal Trade Commission (FTC) and other federal regulatory agencies to enforce the restrictions and requirements in the bill and to issue regulations related to the security of consumers' personal information.

Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and a total of $5 million over the 2006-2011 period. Enacting the bill would not have a significant impact on direct spending or revenues.

H.R. 3997 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA); but CBO estimates that the aggregate cost of complying with those mandates would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

H.R. 3997 would impose private-sector mandates, as defined in UMRA, on financial institutions, employers, consumer credit-reporting agencies and other entities that engage in assembling or evaluating consumer financial information using any means or facility of interstate commerce. While CBO cannot determine the total direct costs of complying with each mandate, the security standards and notification requirements in H.R. 3997 would impose compliance costs on a large number of private-sector entities. Based on this information, CBO estimates that the aggregate direct cost of mandates in the bill, could

exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

## ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 3997 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

| | By Fiscal Year, in Millions of Dollars | | | | | |
|---|---|---|---|---|---|---|
| | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 |
| **CHANGES IN SPENDING SUBJECT TO APPROPRIATION [a]** | | | | | | |
| Estimated Authorization Level | * | 1 | 1 | 1 | 1 | 1 |
| Estimated Outlays | * | 1 | 1 | 1 | 1 | 1 |

NOTE: * = less than $500,000.

a. Enacting H.R. 3997 would also have small effects on direct spending and revenues, but those effects would be less than $500,000 a year.

## BASIS OF ESTIMATE

CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and about $5 million over the 2006-2011 period to issue regulations and enforce the bill's new provisions regarding the security of consumers' personal information. For this estimate, CBO assumes that the bill will be enacted before the end of 2006, that the estimated amounts will be appropriated for each year, and that outlays will follow historical spending patterns. Enacting the legislation would not have a significant effect on direct spending or revenues.

### Spending Subject to Appropriation

H.R. 3997 would require that private companies take certain steps to safeguard consumers' personal information. Private companies also would be required to investigate and remedy security breaches and to notify consumers and certain authorities in the event of a breach. Under the bill, consumers would have the option to freeze their credit reports in the event of a threat to the security of their personal information. The Federal Trade Commission, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal

Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), the Office of Federal Housing Enterprise Oversight (OFHEO), and the Federal Housing Finance Board (FHFB) would enforce the restrictions and requirements under the bill and create regulations related to the security of consumers' personal information.

Based on information provided by the FTC, CBO estimates that implementing H.R. 3997 would cost less than $500,000 in 2006 and $5 million over the 2006-2011 period for the FTC to develop and issue regulations and to enforce the bill's provisions related to information security. Those costs would be subject to the availability of appropriated funds. CBO estimates that implementing the bill would not have a significant impact on spending subject to appropriation for the other regulatory agencies.

**Direct Spending and Revenues**

Enacting H.R. 3997 would affect direct spending and revenues because of provisions affecting financial regulatory agencies and civil penalties. CBO estimates that any such effects would not be significant.

H.R. 3997 would require several financial regulatory agencies to enforce the regulations on the security of consumers' personal information as they apply to financial institutions: OCC, FDIC, the Federal Reserve, the NCUA, and OTS. Any additional direct spending by NCUA, OCC, and OTS to implement the bill would have no net budgetary impact because those agencies charge annual fees to cover all of their administrative expenses. In contrast, the FDIC's sources of income—primarily intragovernmental interest earnings and insurance premiums—do not change in tandem with in its annual expenditures; as a result, any added costs would increase direct spending unless and until the FDIC raised insurance premiums to offset those expenses. Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts).

According to FDIC officials, enacting H.R. 3997 would not have a significant effect on their workload or budgets. For this estimate, CBO assumes that the FDIC would not assess additional premiums to cover the small costs associated with implementing this bill. Thus, CBO estimates that enacting this bill would increase direct spending and offsetting receipts of the NCUA, OTS, OCC, and FDIC by less than $500,000 a year. Based on information from the Federal Reserve, CBO estimates that enacting H.R. 3997 would reduce revenues by less than $500,000 a year.

Enacting H.R. 3997 could increase federal revenues as a result of the collection of additional civil penalties assessed for violation of laws related to information security. Collections of civil penalties are recorded in the budget as revenues. CBO estimates, however, that any additional revenues that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

## ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

H.R. 3997 contains intergovernmental mandates as defined in UMRA because it would require state entities that regulate insurance to enforce certain administrative rules and would explicitly preempt laws in about 20 states that regulate the protection and use of certain personal data. Based on conversations with state and local governments and a review of current legal precedents, CBO assumes that intergovernmental entities would not be required to comply with new data security and notification requirements contained in the bill. CBO estimates, therefore, that the aggregate cost to intergovernmental entities of complying with the mandates in the bill would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

## ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 3997 would impose private-sector mandates, as defined in UMRA, on financial institutions, employers, consumer credit-reporting agencies, and other entities that engage in assembling or evaluating consumer financial information using any means or facility of interstate commerce. Each entity would be required to protect "sensitive financial personal information" relating to any consumer against unauthorized access that is reasonably likely to result in harm or inconvenience and to provide notice to consumers of data security breaches. The legislation defines sensitive financial personal information as a combination of sensitive financial identity information (name, address, or phone number with Social Security number, driver's license number, or other personal identification information), or sensitive financial account information (financial account number with information allowing access to the account), or both.

In addition, the bill would require the Secretary of the Treasury, the Federal Reserve System, the Federal Trade Commission, and certain other federal regulatory agencies to jointly develop standards and guidelines to implement data security safeguards. Because those standards and regulations have not been issued, CBO cannot determine the total direct costs of complying with those mandates, however, certain mandates in H.R. 3997 would impose compliance costs on a large number of private-sector entities. Based on this information, CBO estimates that the aggregate direct cost of the mandates could exceed the annual

threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

**Protection of Sensitive Financial Personal Information**

Section 2 would require certain private companies to implement and maintain reasonable measures to protect the security and confidentiality of sensitive financial personal information, including the proper disposal of such information. Such companies would include consumer reporting agencies, financial institutions, businesses, employers, and other entities that assemble or evaluate sensitive financial personal information using any means or facility of interstate commerce. The cost of this mandate would depend on both the number of covered entities and the average cost to an entity of complying with the mandates. According to industry sources, generally all consumer reporting entities have some measure of security in place. But because standards and regulations have not been issued, CBO does not have enough information to determine the incremental cost for such entities to comply with the mandate.

**Notification of Security Breach**

Section 2 also would require certain private entities to comply with certain procedures for notifying the Secret Service, regulatory agencies, affected third parties, and consumers if a security breach involving sensitive financial personal information has occurred, is likely to have occurred, or is unavoidable. In addition, the bill would require consumer reporters to:

- Investigate any suspected breach of security;
- Notify credit reporting agencies if the breach affects 1,000 or more consumers;
- Take prompt and reasonable measures to repair a breach of security and restore the integrity of the security safeguards; and
- Delay the release of any security breach notification if requested by law enforcement.

If an entity becomes aware that a security breach is reasonably likely to have occurred or is unavoidable, they would be required to provide a specific notification to any affected consumer. Any entity required to provide such notification also would be required to offer affected consumers free credit-file monitoring and identity-monitoring services for at least six months.

The cost of this mandate depends on the number of security breaches that occur, the average number of persons affected by a breach, and the cost per person for notification and credit-file monitoring. According to several industry sources, over 100 security breaches involving sensitive information occurred in 2005, but generally only the largest of breaches are noticed and recorded. Nevertheless, available information suggests that security breaches are not rare. Although the cost to notify individuals and other entities in the event of a security breach may be small per person, the potentially large number of people in data systems maintained by some private companies would make the cost of notification and monitoring associated with one breach significant. Furthermore, certain companies do not maintain the mailing addresses of customers for whom they have name and credit card information. It would be costly for those entities to begin keeping that information. While the regulations regarding consumer notification have not been issued, CBO expects that the cost imposed on consumer reporting entities by the notification requirements could be large relative to the annual threshold established by UMRA for private-sector mandates.

### Credit Report Security Freeze

Section 2 also would allow consumers who have been the victim of identity theft to place a security freeze on their credit report by making a request to a consumer credit-reporting agency. The consumer reporting agency would be prevented from releasing the credit report to any third parties without a prior express authorization from the consumer. The agency also would be required to send a written confirmation of the security freeze to the consumer within 10 business days and provide a unique personal identification number or password to be used to authorize the release of any reports. According to industry sources, the major credit-reporting agencies currently provide a security freeze for consumers and have the systems and procedures in place to accept, impose, and release freezes on credit reports. Therefore, CBO expects that the incremental cost to comply with this mandate would be minimal.

## PREVIOUS CBO ESTIMATES

On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005. On March 10, 2006, CBO transmitted a cost estimate for S.1326, the Notification of Risk to Personal Data Act, as reported by the Senate Committee on the Judiciary on October 20, 2005. H.R. 3997, S. 1408, and S. 1326 would require private companies to take certain precautions to safeguard the personal information of consumers. S. 1326 contains similar requirements for government agencies. S. 1408 would specifically authorize the appropriation of $5 million over the 2006-2010 period for the FTC to enforce

the restrictions and requirements under that bill, while H.R. 3997 would not specifically authorize appropriations for the FTC. However, based on information provided by the FTC, we estimate that spending subject to appropriation would be similar under H.R. 3997 and S. 1408. Because S.1326 also would require government agencies to comply with provisions related to data security, we estimate that spending subject to appropriation would be higher under S. 1326 as compared to the other bills. None of the bills would have a significant impact on direct spending or revenues.

S. 1408 would impose private-sector mandates on certain private entities and consumer credit-reporting agencies that acquire, maintain, or utilize sensitive personal information. S. 1326 would impose private-sector mandates on certain private entities that own or license computerized data containing sensitive personal information. S. 1408 also includes a provision to allow consumers to place a security freeze on their credit report. Since the bills would impose security standards and notification requirements on a large number of private-sector entities, CBO estimated that the total direct cost of mandates in those bills would exceed the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

**ESTIMATE PREPARED BY:**

Federal Costs: Melissa Z. Petersen and Kathleen Gramp
Impact on State, Local, and Tribal Governments: Sarah Puro
Impact on the Private Sector: Paige Piper/Bach

**ESTIMATE APPROVED BY:**

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis